

EXCLUSIVE: An Interview With IBM Chairman John F. Akers

DATA MATION

FOR MANAGERS OF INFORMATION TECHNOLOGY WORLDWIDE

The Rise of an Information Utility

IBM Wants to Satisfy
Every IS Need...
Will Users Plug In?



Also in this issue:
Dialing for PC Software Support
Managing Computer Security
Networking: An Alternative to NFS

DATAMATION®

FOR MANAGERS OF INFORMATION TECHNOLOGY WORLDWIDE



The Rise of an Information Utility 26

BY RALPH EMMETT CARLYLE AND JEFF MOAD The revamped, reorganized, redeployed IBM attempts to be all things to all users: Ultimate Consultant, Premier Integrator, Super Service Company—perhaps the world's first Information Utility? The costs and benefits to users of plugging into this SAA-grounded utility are hard to calculate, yet fundamentally simple: IBM will provide them with the high-level business interfaces they seek in exchange for being given the role of technical manager and business consultant/integrator.

Cover Photography by Walter Wick

DEPARTMENTS

Inside DATAMATION	4
Letters and Access	6
Look Ahead	11
Frito-Lay adds OS/2 crunch to decision support.	
New Products	70
Motorola's factory automation is for real time.	
Information Economics	72
Opinion	74
Planner	75
Career Opportunities	76
Company Index	84
Ad Index	84



THE COMPETITION

IBM Redefines the Competition 37

BY GARY McWILLIAMS AND SUSAN KERR IBM's push into value-added services, systems integration, and consulting adds EDS, Arthur Andersen, and Price Waterhouse to Big Blue's crowded field of competitors. Their struggle is for nothing less than the hearts and minds—not to mention budgets—of IS users intent on creating integrated computing environments dedicated to running their businesses.

How One Contract Was Structured 38

THE RELATIONSHIPS

IBM Mends Third-Party Fences 41

BY BOB FRANCIS AND WILLIE SCHATZ Big Blue is relying on third-party software developers and resellers to help it bring solutions to certain markets and to carry off its Systems Application Architecture strategy. But can it really support indirect sales?

Who'll Pay the Price for IBM's Protection? 42

Network Partners 44

EXCLUSIVE

THE VISION

All Things to All Customers 46

BY RALPH EMMETT CARLYLE AND TIM MEAD IBM chairman John F. Akers wants his company to compete in nearly every corner of the world's IS business, he tells DATAMATION in an exclusive interview. If it means going against established systems integrators like EDS, fine. If it means settling for just a piece of the action, that's okay, too.

SOFTWARE

SUPPORT

Dialing for HELP 53

BY EDWARD J. JOYCE As the PC software field narrows, customer support is becoming more competitive as users demand better, faster, and more service than ever before. The telephone hot line is becoming a major weapon in software competition.

SYSTEMS

INTEGRATION

The Great Australian Tax Deal 59

BY NORMAN KEMP Four mainframe system vendors are vying for a \$600 million nationwide tax automation project, Australia's largest systems integration deal ever. The project entails linking large and disparate financial databases via the mainframes and 10,000 workstations.

COMMUNICATIONS

NETWORKING

IBM's NFS Alternative 63

BY SUSAN KERR IBM is expending a considerable amount of money and development energy to bring its Unix-based distributed computing system—the Andrew File System—into the commercial world to vie with the industry-standard Network File System.

MANAGEMENT

SECURITY

Managing Computer Security 67

BY ALI F. FARHOOMAND AND MICHAEL MURPHY A recent survey of Fortune 500 companies has found that while major industrials are very concerned about security, they are not necessarily practicing what their security officers are preaching. There is a lot of room for improvement, especially in the realm of personnel security.

A Computer Security Framework 68

INTERNATIONAL

Special supplement, not included in all issues.

68-1

Is the New IBM Listening to You?

January 1 has become an important date on DATAMATION's editorial calendar. For the past four years, it has been the date of the issue in which we feature an in-depth examination of IBM. In a world of emerging standards, vast information networks, and all-encompassing architectures, knowing what the world's largest IS supplier is doing, and why, is crucial for users of information technology products and services.

Over the past several years, IBM has gone through a metamorphosis. Internal reorganization and redeployment, revamping of its three major product lines, and the introduction of SAA have combined to fashion a new company, one trying to be intentionally focused on the customer and the market. And so, DATAMATION has applied the power of its entire writing staff—nearly 100 years of combined computer industry editorial experience—to bringing into focus the identity and mission of IBM.

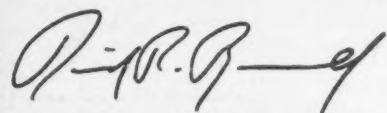
In September, we began the process with a two-day editorial meeting of 12 writers and editors. This meeting was followed up by five international conference calls among the staff even as the process of reporting—including interviews both by phone and in person with IBM executives and scores of IBM customers and analysts—took its course. The result: a four-part series that puts into perspective what IBM is doing, how it is doing it, and what it means for you, the user.

The first article in the series, "The Rise of an Information Utility," p. 26, is an analysis and interpretation of the new IBM and its attempt to become the all-encompassing provider of IS products and services. Teaming up on this article were Ralph Emmett Carlyle, a 12-year DATAMATION veteran known for his powers of synthesis, and Jeff Moad, who for the past 10 years has been reporting on the computer industry (the last three as DATAMATION's San Francisco bureau chief) and whose abilities as a writer are matched only by his relentlessness as a reporter. What they've come up with, we think you'll agree, is perhaps the most penetrating analysis of IBM to be found. Next is an analysis of the competition; how Big Blue's activities as partner, systems integrator, project manager, etc., stack up against the likes of EDS, Unisys, Arthur Andersen, and others. San Jose bureau manager Susan Kerr, a five-year industry veteran who joined DATAMATION in 1986 and is known for cutting to the heart of an argument; and Gary McWilliams, who, with nearly nine years of industry experience, is the dean of New England-based computer journalists, joined to reveal the hands of the other players and the attitudes of customers toward the new IBM.

The third part of our series covers what for IBM is a critical part of its market strategy—third-party software developers. It was written by Dallas bureau chief Bob Francis, who joined DATAMATION last year, and by Washington bureau manager Willie Schatz, an eight-year DATAMATION editor, and six-year veteran international editor Paul Tate; the latter two report on IBM's intellectual property protection activities and overseas partnerships, respectively.

We wrap up with an exclusive interview with IBM chairman John Akers, who tells editor-in-chief Tim Mead and senior writer Carlyle the IBM message: that IBM is listening to customers and will provide them with what they want and need.

After you finish reading our IBM report, you make the call. Is IBM listening to you? Are you getting what you need to run your business? And then take a moment to let us know, either by letter or by phone, your judgment on the new IBM.



—David R. Brousell, Executive Editor



IBM CHAIRMAN AKERS (center) with DATAMATION's Carlyle (left) and Mead.

Photograph by Ken Kerbs

DATAMATION[®]

Editor-in-Chief Tim Mead

Executive Editor David R. Brousell

Managing Editor Parker Hodges

Senior Editor Linda Runyan

International Editor Paul Tate

Art Director Robert L. Lascaro

Senior Writer Ralph E. Carlyle

Section Editors Theresa Barry,

Marsha J. Fisher

Production Editor Hernalee Walker

Production Assistant Suzanne P. White

Copy Chief Jay Blickstein

Copy Editor Rene Matthews

Associate Art Director Anne Cooney

Assistant Art Director Carolee Young

Editorial Assistants Lauren Murphy (London),

Karen J. Scher (New York)

Editorial Secretary Laura Gilette

Bureau Managers

Boston Gary McWilliams

Dallas Robert Francis

London Paul Tate

Los Angeles Tom McCusker

San Francisco Jeff Moad

San Jose Susan Kerr

Washington Willie Schatz

Foreign Correspondents

Eastern Europe David Hebditch (Leeds)

France James Etheridge (Paris)

Italy Janette Martin (Milan)

Contributing Editors Joseph Kelly,

Fred Lamond, Hesh Wiener

Advisory Board Joseph Ferreira, John Imlay,

Angeline Pantages, Russell Pipe, Carl Reynolds

Publishing Director Donald Fagan

Associate Publisher William Segallis

Promotion Manager Stacy Aaron

Production Manager Eric Jorgensen

Research Manager Laraine Donisi

Director of Production Robert Elder

Director of Art Department Barrie Stern

Circulation Manager Roxanne Wilson

EDITORIAL OFFICES

Headquarters: 249 W. 17 St., New York, NY 10011.
(212) 645-0067; telex 127703; fax (212) 242-6987. New
England: 199 Wells Ave., Newton, MA 02159, (617) 964-
3730; Washington, D.C.: 4451 Albemarle St. NW, Wash-
ington, DC 20016, (202) 966-7000; Central: 9330 LBJ
Blvd., Suite 1060, Dallas, TX 75243, (214) 644-3683;
Western: 12233 W. Olympic, Los Angeles, CA 90064,
(213) 826-5818; 582 Market St., Suite 1007, San Francis-
co, CA 94104, (415) 981-2595; 3031 Tach Way, Suite
100, San Jose, CA 95128-2593, (408) 243-8838. Inter-
national: 27 Paul St., London EC2A 4JU, England, (44-1)
628-7030, telex 914811; CPO Box 666, Tokyo, Japan,
(81-3) 201-2335, fax 2135053.

DATAMATION (ISSN 0011-6963) Magazine is issued
twice monthly on the 1st and 15th of every month by The
Cahners Publishing Company, A Division of Reed Publishing
USA, 275 Washington St., Newton, MA 02158-1630. Wil-
liam M. Platt, Chief Executive Officer; Terrence M. McCar-
dott, President; Frank J. Sibley, Group Vice President; Jerry
D. Neth, Vice President/Publishing Operations; J.J. Walsh,
Financial Vice President/Magazine Division; Thomas J. Del-
lamaria, Vice President/Production and Manufacturing. Edi-
torial and advertising offices: 249 W. 17th St., New York,
NY 10011. Published at Woodstock, IL. Annual subscrip-
tion rates: U.S. and possessions: \$69; Canada: \$98; Japan,
Australia, New Zealand: \$180 air freight; Europe: \$157 air
freight, \$290 air mail. All other nations: \$157 surface.
\$250 air mail. Reduced rate for U.S. public and school li-
braries: \$47. Single copy: \$10 in U.S. Sole agent for sub-
scriptions in Japan is Maruzen Co. Ltd., 3-10 Nihonbashi,
2-Chome, Chuo-ku, Tokyo 103, J.; sole agent for all other
foreign subscriptions is J.B. Tratsart Ltd., 154 A Greenford
Rd., Harrow, Middlesex HA1 3QT, England, (01) 422-8295
or 422-2456. No subscription agency is authorized by us to
solicit or take orders for subscriptions. Circulation records
are maintained at 44 Cook St., Denver, CO 80206. Phone
(303) 388-4511. Second-class postage paid at Denver, CO
80206 and at additional mailing office. DATAMATION
copyright 1988 by Reed Publishing USA; Saul Goldweitz,
Chairman; Ronald G. Segel, President and Chief Executive
Officer; Robert L. Krafciof, Executive Vice President. All
rights reserved. DATAMATION is a registered trademark of
Cahners Publishing Co. Reprints of articles are available;
contact Frank Pruzina (312) 636-8900. Microfilm copies of
DATAMATION may be obtained from University Micro-
films, A Xerox Company, 300 N. Zeeb Rd., Ann Arbor, MI
48106. Printed by Graftek Press Inc. All inquiries and re-
quests for change of address should be accompanied by mail-
ing label from latest issue of magazine. Allow two months for
change to be made. POSTMASTER: send address changes
to DATAMATION, 44 Cook St., Denver, CO 80206.

Managing Computer Security

MANAGEMENT
SECURITY

Everyone is concerned about security, but firms don't always practice what their security officers preach. A recent survey of Fortune 500 companies reveals there is room for improvement, especially in the personnel security department.

BY ALI F. FARHOOMAND AND MICHAEL MURPHY

Amidst a lip-service overload about PC proliferation and computer security, few empirical studies have been made of computer fraud, crime, and abuse, computer security control and audit, and the cost of security. The few studies that have been performed have not compared the way firms actually manage their computer security with the way they admit they should.

Recently, we surveyed the Fortune 500 firms to gain insight into the nature of various elements of computer security management. An attempt was made to investigate relationships between the prevailing computer security problems and the size of a company's information systems facilities, as measured by the number of MIS employees and the annual budget of the MIS department.

The surveys were mailed to computer security officers or MIS managers of all the Fortune 500 companies. The question-

naire inquired about various aspects of computer security. Within six weeks, 88 out of 500 surveys were returned, and 86 were deemed usable. The response rate (17.2%) appeared reasonable in light of the sensitive nature of the topic.

The median number of employees in the surveyed MIS departments was found to be approximately 150 people. The median annual MIS budget of the responding companies was estimated to be approximately \$20 million. More than half of the respondents allocate less than 0.5% of this to computer security; about a third allocate between 0.5% and 1.0%; and the remaining companies allocate over 1.0%.

For questions of policy direction, standards and procedures, and areas of responsibility, the surveyed firms usually have comprehensive guidelines in place. More than three quarters of the firms have documented emergency, backup, and recovery plans. However, approximately

one third of the firms never test these plans, nor do they reevaluate security programs at specified intervals.

Policies are generally formulated by consultation between the MIS manager and top management. Before computer security policies can be adopted, final approval must be obtained from senior management. This involvement in both policy formulation and approval can be viewed as a definite sign that top management provides a high level of support to the computer security program.

Personnel Security Weak

Personnel security programs were found to be weak: companies do not generally do a good job of checking up on employees once they have begun to perform their duties. In particular, firms do not:

- use attitude surveys to monitor the level of employee morale;
- consider an employee's level of security consciousness during his/her performance assessment;
- use job rotation as a means of evaluating an employee's security-related behaviors;
- use the regular vacation of a key employee to perform a mini-audit of that employee's work; and
- identify employees whose particular responsibilities make them potential security risks.

To understand why firms have not adopted these measures, it is instructive to examine the relationship between employees and the personnel department. At the pre-employment stage, background investigations and reference checks of prospective employees are performed as a matter of course; pre-employment agreements are signed with new employees; and new employees are formally notified of their security responsibilities. This interaction facilitates the personnel security program. During the post-employment



Illustration by Karen Stolper

Problems Affecting Computer Security

Computers are KO'd by man and nature.

PROBLEM	% FIRMS AFFECTED
Utilities failure	80.8
Inadequate control	75.6
Compliance failure	73.1
Improper guidance	67.9
Environment support breakdown	64.1
Electromagnetic discharges	43.6
Liquids	29.5
Electronic intrusion	29.5
Fraud and embezzlement	16.7
Gases	11.5
Extreme temperature	11.5
Physical intrusion	10.3
Service loss	7.7
General violence (vandalism)	7.7
Specific violence (sabotage)	6.4
Living organisms	2.6
Projectiles	2.6
Earth movements	1.3

Source: Ali F. Farhoomand

stage there is again a substantial amount of contact between personnel officers and departing employees. However, during the employment stage of the employment cycle, the survey shows that most elements of the personnel security program are neglected by the majority of firms.

Security training is another weak area in the personnel security program, with 52% of firms making no provision for any form of employee security training.

Slightly more than half of the firms have developed asset-threat inventories—inventories that address what safeguards will protect their assets against predetermined threats. The most commonly used measures that firms employ to rank identified threats are expected loss, frequency of occurrence, hours of downtime, and dollars of damage.

The rest of the firms neither perform any risk assessment of security threats nor do they formally identify and evaluate their computer assets. Subjective methods of risk assessment are more widely

employed in identifying assets and evaluating potential threats than such quantitative methods as the Delphi technique or Threat Model (an analysis tool for identifying security threats that is based on cause and effect relationships). As one of the respondents commented, "Risk analysis need not be performed to know that software security systems are required. In fact, such analyses only prove what is already known and, thus, amount to wasted time and effort."

Security Officers' Views

Although there is a general congruence between how firms manage computer security and how their security officers feel computer security should be managed, some differences were reported. Particularly in the area of personnel security, the respondents felt that their firms are failing in two important areas: providing some form of security training for MIS employees and identifying employees whose particular responsibilities make them potential security risks.

In addition, there are a series of minor differences between the views of security officers and the firms' practices in the area of asset-threat inventory. Most of these differences relate to either the formality of the analysis and control procedures or the importance of applying certain security programs. For the most part, the firms use subjective estimates made by people who are familiar with the assets, while security officers prefer using estimates based on the cost created if the asset were unavailable for a specified time period.

Overall, security officers feel that still more can be done to enhance the level of computer security within their firms, and they recommend applying more formal analysis and control procedures to security programs, as well as increasing the frequency of certain security procedures.

The problems that have affected the largest number of firms are summarized and shown in "Problems Affecting Computer Security." The costliest are utilities failures, according to 36% of the firms; compliance failure, in 33% of the firms; and improper guidance, in 21% of the firms. These findings suggest that the often publicized threats such as computer hackers and other white collar criminals have had either little or no effect on the majority of firms, or are not being reported.

Ali F. Farhoomand is an assistant professor of MIS at Concordia University in Montreal. Michael Murphy is a systems engineer with Canadian National in Montreal.

A Computer Security Framework

We based our Fortune 500 survey of computer security management techniques on the Total Computer Security Concept that was presented by L.H. Fine in *Computer Security—A Guide for Management* (Heinemann, London, 1983). Fine divides the issues related to the computer security architecture of a company into two categories: management issues and technical issues. The management issues ultimately are the responsibility of senior management, while the technical issues are clearly the responsibility of MIS management.

The technical issues surrounding a firm's computer security are threefold: physical security, controls, and system security. The issues that concern management fall into five categories:

A defined and documented computer security policy. This specifies the scope and direction of the company's involvement in computer security.

Standards and procedures. These are the detailed, day-to-day guidelines that should be followed during any type of MIS operation or activity. They are designed to help protect the firm's computing assets from most security threats.

An outline of responsibility for computer security. This involves division of responsibility among the computer security function, the MIS department, the personnel department, and top management.

A personnel security program. This includes employees' entire employment cycle, from pre-employment to post-employment. This program should also address such areas as pre-employment screening, condition of employment agreements, security training, employee morale, and employee termination procedures.

A complete asset-threat inventory. This provides a set of safeguards designed to protect a firm's computing assets against a group of predetermined potential threats. The inventory includes: identification and valuation of the assets; identification of the potential threats; risk assessment process; identification of the potential safeguards; selection of safeguards; adoption of contingency plans; testing of contingency plans; auditing of the computer system; and ongoing computer security evaluation.

Fine's Total Computer Security Concept can be envisaged as a horizontal beam supported by eight pillars: the five management issues and the three technical issues. This beam supports the integrity and confidentiality of the firm's information systems.